REMARKS

Applicant appreciates the Examiner's attention to this application.

This response amends claims 12 and 23 to correct minor informalities; amends claims 12, 14, 16, 20, and 23 to clarify which elements perform which operations; cancels claims 25-29; and enters new claims 30-34. Claims 1, 9, 12, 14, 20, 23, 30, and 33 are the pending independent claims.

Reconsideration of the present application in view of the enclosed amendments and remarks is respectfully requested.

ARGUMENT

The Office Action rejects all of the original claims based on 35 U.S.C. § 103(a). Applicant respectfully traverses those rejections.

Claims 1-3, 12-16, and 23-24

The Office Action rejects claims 1-3, 12-16, and 23-24 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent no. 6,442,686 to Mark J. McArdle et al. (hereinafter "McArdle"), in view of U.S. patent no. 6,253,322 to Seiichi Susaki et al. (hereinafter "Susaki").

McArdle pertains to a method for enforcing security policies through use of a "policy management agent." Specifically, the policy management agent is interposed between clients and a standard mail server, and the policy management agent monitors intercepts email from the clients before the email reaches the mail server, to enforce email security policies. (Abstract.)

Susaki pertains to a method for archiving electronic contracts. The contracts are archived or escrowed by a system referred to as a "service providing unit." Specifically, when two (or more) parties want to enter into a contract that is memorialized in electronic or digital form, those parties (which Susaki refers to as "service receiving units") electronically sign the electronic contract and then send the signed copies to the escrow service (i.e., to the service providing unit). The service

providing unit then consolidates the contracts into a single document, signs that document, and archives that document. The service providing unit thus serves as an escrow agent for electronic contracts.

By contrast, the present application pertains to methods and systems for monitoring encrypted communications in a network. For instance, claim 1 recites a method involving a "policy administrator" that establishes a "network monitoring digital contract" with a "network monitoring element." As explained on pages 7-9 of the Detailed Description, a network monitoring digital contract memorializes an agreement between the policy administrator and the network monitoring element to authorize the network monitoring element to monitor communications between network elements. In addition, claim 1 recites that the policy administrator provides the network monitoring element with decrypting information, based on (a) the network monitoring digital contract between the policy administrator and the network monitoring element and (b) a "network use digital contract" between the policy administrator and first and second "network elements." The decrypting information that the policy administrator sends to the network monitoring element allows the network monitoring element to "decrypt encrypted communications between the first network element and the second network." Claim 14 involves software for implementing features such as those recited in claim 1.

Neither McArdle nor Susaki provide any motivation for combining an escrow agent for electronic contracts with a policy management agent for email. Furthermore, even if McArdle and Susaki were to be combined, the combination would merely create a data processing system that (a) serves as an escrow agent for archiving digital contracts from service receiving units, while also (b) serving as an email monitor, to intercept email messages and enforce security restrictions. The combination would not disclose or suggest the present invention.

For example, the combination would not disclose or suggest a "policy administrator" that establishes a "network monitoring digital contract" with a "network monitoring element." Page 17 of the Office Action seems to recognize this fact, when stating that "McArdle and Susakie [sic] does not expressly disclose a network

monitoring element establishing a network monitoring digital contract with a policy administrator."

Furthermore, a combination of McArdle and Susakie would not disclose or suggest the policy administrator supplying the network monitoring agent with decrypting information, based on the network monitoring digital contract, where the decrypting information allows the network monitoring element to decrypt communications between first and second network elements.

Claim 12 involves a first network element that (a) establishes a network use digital contract with the policy administrator, (b) logs decrypting keys used for communications with a second network element under the network use digital contract, and (c) "permits the policy administrator to access the log to obtain the decrypting keys." Claim 23 involves software for implementing features such as those recited in claim 12.

A combination of McArdle and Susaki would not disclose or suggest a network element that logs decrypting keys and then allows a policy administrator to obtain the decrypting keys from the log, in accordance with a network use digital contract between the policy administrator and the network element.

For reasons including those set forth above, the Office Action fails to make out a *prima facie* case of obviousness for independent claims 1, 12, 14, and 23. Claims 2-3, 13, 15-16, and 24 each depend ultimately from one of those independent claims. The Office Action therefore fails to make out a *prima facie* case of obviousness for claims 1-3, 12-16, and 23-24.

Claims 4-11 and 17-19

The Office Action rejects claims 4-11 and 17-19 under 35 U.S.C. § 103(a) as being unpatentable over McArdle and Susaki, in view of U.S. patent no. 6,324,645 to Richard F. Andrews et al. (hereinafter "Andrews").

Andrews pertains to a method for managing a "public key infrastructure," such as the infrastructure used by a certification authority (CA) for managing and authenticating digital certificates (col. 6, lines 35-43). In particular, Andrews pertains to a method for controlling access to the infrastructure, based on digital certificates

associated with users of the infrastructure. For instance, Andrews discloses a process for creating a digital certificate for a user, in which an "access label" is included in the digital certificate to identify access rights for the user (col. 12, lines 24-44).

McArdle, Susaki, and Andrews do not provide a motivation for combining (a) an escrow agent for electronic contracts, (b) a policy management agent for email, and (c) a method for controlling access to a public-key management infrastructure. Furthermore, even if McArdle, Susaki, and Andrews were to be combined, the combination would merely create a data processing system that (a) allows service receiving units to escrow digital contracts, (b) monitors email messages to enforce security restrictions, and also (c) creates digital certificates that include includes access labels which identify access rights within a public-key management infrastructure. The combination would not disclose or suggest the features discussed above with regard to independent claims 1, 12, 14, and 23.

In the present application, claims 4-8 depend from, and therefore implicitly include the features of, claim 1. Likewise, claims 17-19 depend from, and therefore implicitly include the features of, claim 14. Since a combination of McArdle, Susaki, and Andrews would not render the respective independent claims obvious, the Office Action fails to make out a *prima facie* case of obviousness for claims 4-8 and 17-19.

Claims 10 and 11 of the present application depend from claim 9. Claim 9 pertains to a method in which the network monitoring element establishes a "network monitoring digital contract" with the policy administrator. The network monitoring element also obtains decrypting information from the policy administrator, as per terms in the network monitoring digital contract. The decrypting information allows the network monitoring element to decrypt "encrypted communications between a first network element and a second network element."

A combination of McArdle, Susaki, and Andrews would not disclose or suggest those features. The Office Action therefore fails to make out a *prima facie* case of obviousness for claims 9-11.

Claims 20-21

The Office Action rejects claims 20-21 under 35 U.S.C. § 103(a) as being unpatentable over McArdle, in view of Andrews. Claim 21 depends from claim 20. Claim 20 involves software for implementing features such as those recited in claim 9, such as features for establishing a "network monitoring digital contract" with a policy administrator, and for obtaining decrypting information "from the policy administrator." Claim 20 also recites using the decrypting information "at a network monitoring element" to decrypt encrypted communications "between a first network element and a second network element," in accordance with "terms in the network monitoring digital contract."

A combination of McArdle and Andrews would not disclose or suggest those features. The Office Action therefore fails to make out a *prima facie* case of obviousness for claims 20-21.

Claim 22

The Office Action rejects claim 22 under 35 U.S.C. § 103(a) as being unpatentable over McArdle and Andrews, in view of Susaki. Claim 22 depends from claim 20. Claim 20 is discussed in the two paragraphs immediately above. A combination of McArdle, Andrews, and Susaki would not disclose or suggest the features of claim 20. Since claim 22 implicitly includes the features of claim 20, the Office Action fails to make out a *prima facie* case of obviousness for claim 22.

Claims 25-27 and 30-32

The Office Action rejects claim 25-27 under 35 U.S.C. § 103(a) as being unpatentable over McArdle, in view of U.S. patent no. 6,336,186 to Marc D. Dyksterhouse et al. (hereinafter "Dyksterhouse"). To the extent that these rejections might be applied to claims 30-32, Applicant respectfully traverses.

Claims 31 and 32 depend from claim 30. Claim 30 involves an apparatus to implement features such as those recited in claim 1. The apparatus, for instance, is able to (a) establish a "network monitoring digital contract" with a "network monitoring element," (b) establish "network use digital contracts" with first and

second network elements, and (c) transmit decrypting information "to the network monitoring element" for decrypting encrypted communications "between the first network element and the second network element" in accordance with terms in the network monitoring digital contract and the network use digital contracts.

By contrast, Dyksterhouse pertains to a server for storing key or certificates. In particular, the "Certificate Server" allows a client to "submit and retrieve keys from a database," based on a set of policy constraints for the client's site or company. (Abstract.) McArdle is discussed above.

Even if McArdle and Dyksterhouse were to be combined, the combination would not disclose or suggest the features quoted above from claim 30. The combination therefore would not render claims 30-32 obvious.

Claims 28-29 and 33-34

The Office Action rejects claim 28-29 under 35 U.S.C. § 103(a) as being unpatentable over Susaki, in view of Dyksterhouse. To the extent that these rejections might be applied to claims 33-34, Applicant respectfully traverses.

Claim 34 depends from claim 33. Claim 33 involves an apparatus to implement features that include (a) establishing a "network monitoring digital contract" with a "policy administrator;" (b) transmitting, to the policy administrator, a "request to monitor encrypted communications between first and second network elements;" and (c) receiving "decrypting information ... from the policy administrator." The decrypting information allows the apparatus to decrypt encrypted "communications between the first and second network elements," in accordance with the terms in the network monitoring digital contract.

Even if Susaki and Dyksterhouse were to be combined, the combination would not disclose or suggest the features quoted above from claim 33. The combination therefore would not render claims 33-34 obvious.

Additional Recited Features

Moreover, the claims recite additional features that are not disclosed or suggested by the cited art. For instance, claim 2 pertains to an embodiment in

which the network monitoring element sends requests to the policy administrator, and the policy administrator sends the network monitoring element "decrypting keys to decrypt the encrypted communications between the first network element and the second network element." Claim 3 pertains to an embodiment in which the policy administrator decrypts the encrypted communications between the network elements, and transmits the decrypted communications to the network monitoring element, per terms in the network monitoring digital contract. Claim 5 recites that the network monitoring digital contract is associated with a limited time period of validity.

For reasons including those set forth above, the Office Action fails to make out a *prima facie* case of obviousness for any of the pending claims.

For these and other reasons, all pending claims are allowable.

CONCLUSION

In view of the foregoing, claims 1-24 and 30-34 are all in condition for allowance.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 732-3927. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: 7/9/04

Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 314-0349

c/o Blakely, Sokoloff, Taylor &
Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026